

25 JUL 2000



PCI/EROO/02075

REC'D 08 SEP 2000

WIPO

PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

EROO/02075

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 21 JUIN 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

This Page Blank (uspto)



REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie

Cet imprimé est à remplir à l'encre noire en lettres capitales

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Réservé à l'INPI

DATE DE REMISE DES PIÈCES **20 JUIL 1999**
N° D'ENREGISTREMENT NATIONAL **9909396**
DÉPARTEMENT DE DÉPÔT **75 INPI PARIS**
DATE DE DÉPÔT **20 JUIL 1999**

1. NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE
**SOCIETE DE PROTECTION
DES INVENTIONS
3, rue du Docteur Lancereaux
75008 PARIS**

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention

☐ demande divisionnaire

☐ certificat d'utilité

☐ transformation d'une demande
de brevet européen

☒ demande initiale

☐ brevet d'invention

n° du pouvoir permanent

références du correspondant

téléphone

**SP16186.C/RS 01 53 83 94 01
C/03059**

date

Établissement du rapport de recherche

☐ différé

☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui

☐ non

Titre de l'invention (200 caractères maximum)

**PROCEDE DE REALISATION D'UNE TRANSACTION ELECTRONIQUE UTILISANT
PLUSIEURS SIGNATURES.**

3 DEMANDEUR (S) n° SIREN

code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

FRANCE TELECOM

LA POSTE

Forme juridique

Société Anonyme

Nationalité (s) **Française**

Adresse (s) complète (s)

6 Place d'Alleray 75015 PARIS

Pays

France

**4 Quai du Point du Jour 92777 BOULOGNE-BILLANCOURT
CEDEX**

France

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui

☒ non

Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois

☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS

antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire)

**D. DU BOISBAUDRY
CPI 950 1304**

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg SP 16186.C/RS
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

99 093 96

TITRE DE L'INVENTION :

PROCEDE DE REALISATION D'UNE TRANSACTION ELECTRONIQUE UTILISANT
PLUSIEURS SIGNATURES.

LE(S) SOUSSIGNÉ(S)

D. DU BOISBAUDRY
c/o SOCIÉTÉ DE PROTECTION
DES INVENTIONS
3, rue du Docteur Lancereaux
75008 PARIS

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

REMERY Patrick

43, rue de Cornouailles
14000 CAEN

De SOLAGES Aymeric

6 rue de la Haie Vigné
14000 CAEN

TRAORE Jacques

84, rue Abbé Lecornu
61100 FLERS

FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur(s) ou du mandataire

PARIS LE 20 JUILLET 1999

D. DU BOISBAUDRY
CPI 950 304

**PROCEDE DE REALISATION D'UNE TRANSACTION
ELECTRONIQUE UTILISANT PLUSIEURS SIGNATURES**

DESCRIPTION

5

Domaine technique

La présente invention a pour objet un procédé de réalisation d'une transaction électronique utilisant plusieurs signatures.

10

Elle trouve une application dans toutes les transactions (téléachat, télépaiement, accès à un service, etc...) s'effectuant à l'aide de moyens électroniques, comme les cartes à puces par exemple. L'invention trouve une application particulière dans le

15

porte-monnaie électronique.

Etat de la technique antérieure

La sécurité des transactions électroniques par carte à puce repose sur des techniques cryptographiques. Le processeur de la puce calcule et émet une signature numérique de la transaction qui constitue une preuve de l'accord de la partie émettrice de la signature sur cette transaction. Cette preuve est spécifique à l'organisme émetteur gestionnaire de l'application. Cette signature numérique est le résultat d'un calcul portant sur les données identifiant l'émetteur de la carte, le terminal, le numéro de la transaction, le montant de la transaction et éventuellement le numéro de compte du porteur.

30

Les données sont transmises à l'émetteur de la carte qui effectue les traitements appropriés tels que l'audit de la transaction par vérification de la signature, mise en recouvrement, débit du compte

client, crédit du compte du fournisseur de services, etc...

Dans une des techniques antérieures décrites dans FR-A-2 748 591, la carte produit deux signatures, la première dite "longue" (algorithme à clé publique) et destinée au fournisseur de services, et la seconde, dite "courte" (algorithme à clé secrète) encapsulée dans la première est destinée à l'émetteur. Le prestataire de services vérifie la signature longue, et si le résultat est correct, rend le service commandé et stocke la signature courte. Il transmet à l'émetteur, en fin de journée, les signatures courtes stockées et les données correspondantes.

Ce schéma, s'il a l'avantage d'être simple, pose cependant quelques problèmes lorsque les paiements sont réalisés au moyen d'un porte-monnaie électronique (PME en abrégé). Il est, en effet, parfois nécessaire d'introduire un ou plusieurs acteurs intermédiaires entre les trois parties déjà citées à savoir le porteur, le prestataire de services et l'émetteur, selon les besoins de concentration effectuant des cumuls de valeur électronique.

Une solution consiste à ajouter des moyens intermédiaires appelés SAM ("Secure Application Modules) vérifiant l'une des deux signatures produites par la carte et cumulant la valeur électronique reçue.

Si les SAM intermédiaires étaient capables d'effectuer la même vérification que celle faite par l'émetteur, la sécurité serait dégradée. En effet, si l'algorithme cryptographique utilisé pour produire la signature destinée à l'émetteur de la carte était à clé secrète, la clé de l'émetteur serait placée à des

niveaux de responsabilité inférieurs vis-à-vis de la garantie de la monnaie électrique.

Si la deuxième signature destinée au fournisseur de services était produite par un algorithme à clé publique, alors les SAM intermédiaires seraient, tout
5 comme le fournisseur de services, en mesure d'authentifier n'importe qu'elle transaction émanant d'un PME. Toutefois, dans ce cas de figure, les signatures seraient de taille nettement plus longues et
10 donc plus coûteuses à transférer, à stocker et à vérifier.

La présente invention a justement pour but de remédier à ces inconvénients.

15

Exposé de l'invention

A cette fin, l'invention propose un procédé utilisant plusieurs signatures, avec une chaîne d'encapsulations-décapsulations. On suppose qu'on est
20 en présence d'un réseau de communications (par exemple un réseau téléphonique) reliant des entités susceptibles de communiquer entre elles, avec la contrainte qu'il n'existe pas de canal de communication directe entre deux entités souhaitant communiquer et
25 que les canaux de communication existants peuvent être unidirectionnels.

Une transaction fait intervenir un sous-ensemble d'entités appelées aussi "acteurs", concourant à des titres divers à la réalisation de la transaction. En
30 pratique, ces entités ou acteurs sont constituées par des moyens physiques : terminal, carte, microprocesseur, etc...

Au cours de la transaction :

- 5 ▪ une entité i dispose des moyens nécessaires (E_{ij}) au calcul des cryptogrammes destinés à une entité j , et/ou à la vérification de cryptogrammes en provenance de j ,
- et une entité j dispose également des moyens (E_{ji}) correspondants,

ces moyens E_{ij} et E_{ji} ayant été obtenus au cours de la phase dite d'initialisation (effectuée préalablement et/ou parallèlement à la transaction elle-même). On dira alors que ces deux entités partagent un système de clés noté $K_{ij}=K_{ji}=\{(i, E_{ij}), (j, E_{ji})\}$. Par exemple :

- dans le cas d'un système à clés secrètes, on a :
 $E_{ij}=E_{ji}=S_{ij}$;
- 15 ▪ dans le cas d'un système à clés publiques, on a :
 - pour une communication monodirectionnelle
 $E_{ij}=(S_i, P_i)$, et $E_j=(P_i)$,
 - pour une communication bidirectionnelle
 $E_{ij}=(S_i, P_i, P_j)$, et $E_{ji}=(S_j, P_i, P_j)$.
- 20

Avec cette définition, le système de clés est une notion symétrique par rapport à i et j . En revanche, si l'on note $K_{ij}(m)$ le cryptogramme d'un message m envoyé par i à j , on a $K_{ij}(m) \neq K_{ji}(m)$.

- 25 Dans ces conditions et sous ces hypothèses, une entité source de message "encapsule" (c'est-à-dire renferme) un message dans une suite de cryptogrammes portant sur des cryptogrammes, eux-mêmes portant sur des cryptogrammes, etc... Tous ces cryptogrammes sont
- 30 calculés à l'aide de systèmes de clés que l'entité source partage respectivement avec chacune des entités intermédiaires situées sur le chemin de la

communication. Le cryptogramme global est émis et chaque entité intermédiaire "décapsule" (c'est-à-dire extrait) le cryptogramme qu'elle reçoit avec le système de clés qu'elle partage avec l'entité source, et
5 transmet le cryptogramme restant à l'entité suivante. De proche en proche, le premier cryptogramme calculé parvient à l'entité destinataire qui extrait le message qui lui est destiné à l'aide du système de clés approprié.

10 Selon les besoins de la transaction et les protocoles utilisés, les cryptogrammes calculés peuvent servir à l'authentification des acteurs, à l'authentification de l'origine des messages, ou à la non-répudiation (à l'émission ou à la réception) de ces
15 messages.

Ce procédé suppose l'existence d'un système de gestion des systèmes de clés (qui englobe la génération, la distribution et/ou l'échange de clés nécessaires à l'établissement de communications sûres
20 avec les autres acteurs), mis en oeuvre au cours d'une phase dite d'initialisation. Ce système de gestion de clés peut être quelconque et par exemple consister en une infrastructure à clé publique, avec un protocole de transport de clés associé.

25 Parmi les entités en présence, certaines peuvent jouer le rôle de tiers de confiance. Par exemple :

- dans le cas d'un système à clé publique, il peut s'agir d'une autorité de certification,
- dans le cas d'un système à clé secrète, il peut
30 s'agir d'une entité maître, partageant une clé secrète avec chacune des autres entités, ou certaines d'entre elles seulement.

Une entité peut participer à une transaction à divers titres comme par exemple :

1. assurer un relais de l'information : une entité joue le rôle de relais intermédiaire et pallie ainsi l'absence de canal de communication reliant directement un expéditeur et un destinataire d'un message nécessaire à la transaction ;
2. assurer une désynchronisation : une entité joue le rôle de cache intermédiaire de messages pour le compte d'une autre entité, destinataire réel de ces messages ; cette entité intermédiaire :
 - pallie l'indisponibilité temporaire du destinataire,
 - est conçue pour être sollicitée plus fréquemment que le destinataire et joue le rôle d'interface regroupant les messages et évitant la sollicitation systématique du destinataire.

L'émetteur et/ou le destinataire ont intérêt à l'arrivée des informations à destination. Les acteurs intermédiaires doivent donc être des relais sûrs de cette information. Plusieurs cas sont notamment possibles :

- les acteurs intermédiaires ont également intérêt à l'arrivée des informations à destination. C'est le cas par exemple lorsqu'il s'agit d'un commerçant dans une transaction financière faisant intervenir un client (acteur expéditeur) et le système de gestion du moyen de paiement (acteur destinataire),
- l'expéditeur et/ou le destinataire font confiance aux acteurs intermédiaires pour

l'opération de relaying (mais pas nécessairement pour l'authenticité de l'origine des informations),

- 5 • les acteurs expéditeurs et destinataire font totalement confiance aux acteurs intermédiaires (tiers de confiance),
- les acteurs expéditeur et destinataire ne font pas du tout confiance aux acteurs intermédiaires, et des moyens de non-répudiation à l'émission et à la réception
10 sont mis en place.

De façon précise, l'invention a pour objet un procédé de réalisation d'une transaction électronique à
15 travers un réseau de communication reliant une pluralité d'entités, ce procédé étant caractérisé en ce qu'il comprend les opérations suivantes :

- a) une première entité élabore un premier message rassemblant les données de la transaction et calcule un premier cryptogramme de ce premier message en utilisant un premier système de clés qu'elle partage avec une dernière ($n^{\text{ième}}$) entité ; la première entité associe ensuite à ce premier cryptogramme un deuxième message et calcule un deuxième cryptogramme de l'ensemble
20 en utilisant un deuxième système de clés qu'elle partage avec l'avant-dernière $(n-1)^{\text{ième}}$ entité ; et ainsi de suite ; la première entité associe au $(n-2)^{\text{ième}}$ cryptogramme précédemment obtenu un $(n-1)^{\text{ième}}$ message et calcule un
25 $(n-1)^{\text{ième}}$ cryptogramme de l'ensemble en utilisant un $(n-1)^{\text{ième}}$ système de clés qu'elle partage avec la deuxième entité ; la première
30

entité transmet le dernier cryptogramme calculé à travers le réseau de communication ;

5 b) la deuxième entité reçoit ce dernier cryptogramme, utilise le système de clés approprié pour extraire du $(n-1)^{\text{ième}}$ cryptogramme le $(n-1)^{\text{ième}}$ message qu'il contient, et transmet le $(n-2)^{\text{ième}}$ cryptogramme restant à la troisième entité ; et ainsi de suite ; la $n^{\text{ième}}$ entité reçoit le premier
10 cryptogramme et utilise le système de clés approprié pour extraire le premier message qu'il contient.

Dans cette définition, la "première entité" n'est
15 pas nécessairement l'entité source du message mais elle peut l'être. De même, la "dernière entité" n'est pas nécessairement l'entité destinataire in fine du message mais elle peut l'être. Ainsi, dans le cas particulier précédent, le réseau de communication comprend
20 uniquement des entités partageant un système de clés avec une première entité, la transaction s'effectuant alors entre la première entité, qui est la source du message et la dernière, qui est le destinataire du message.

25 L'encapsulation est alors totale à la source et la décapsulation progressive jusqu'au destinataire.

Dans une variante de mise en oeuvre, l'encapsulation est partagée (ou répartie). Dans ce cas, le réseau de communication comprend un premier
30 groupe d'entités constitué d'une première entité et de $(i-1)$ autres partageant chacune un système de clés avec ladite première entité, et un deuxième groupe d'entités constitué d'une première entité qui est la dernière

entité du premier groupe à savoir l'entité i , et de $(n-i)$ autres. L'entité i partage un système de clés avec chacune de ses $(n-i)$ entités suivantes. Ce procédé comprend deux phases successives :

- 5 - une première phase dans laquelle le message élaboré par la première entité du premier groupe est transmis à la $i^{\text{ème}}$ entité du premier groupe conformément aux opérations a) et b) définies plus haut,
- 10 - une seconde phase dans laquelle le message extrait par la première entité du second groupe est transmis à la dernière entité du second groupe conformément auxdites opérations a) et b).

15 Dans un cas général, on peut combiner les modes de mise en oeuvre qui viennent d'être définis. Ainsi, le réseau de communications peut comprendre un premier groupe d'entités constitué d'une première entité et de $(i-1)$ autres partageant un système de clés avec ladite

20 première entité, un deuxième groupe d'entités constitué d'une première entité, qui est la dernière entité du premier groupe et $(j-i+1)$ autres partageant un système de clés avec ladite première entité du

25 deuxième groupe, un troisième groupe d'entités constitué d'une première entité qui est la dernière entité du deuxième groupe et de $(n-j)$ autres, les $(n-j+1)$ entités de ce troisième groupe partageant un système de clés avec la première entité du premier groupe, ce procédé étant caractérisé en ce que :

- 30 - la première entité du premier groupe effectue les opérations a) définies plus haut, avec les systèmes de clés qu'elle a en commun avec

chacune des autres entités du premier et du troisième groupe,

- les entités du premier groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) définies plus haut,
- la première entité du deuxième groupe effectue les opérations a) avec les systèmes de clés qu'elle a en commun avec chacune des autres entités du deuxième groupe,
- les entités du deuxième groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) définies plus haut,
- les entités du troisième groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b).

La présente invention a également pour objet une application de ce procédé au paiement par porte-monnaie électronique.

20 Description détaillée de modes de mise en oeuvre

L'authenticité des données est obtenue par des techniques mettant en oeuvre des mécanismes de chiffrement, d'authentification ou de signature.

Le terme "signature" utilisé dans la suite désigne des cryptogrammes obtenus aussi bien au moyen de mécanismes de signature basés sur des algorithmes à clé publique (avec recouvrement ou non du message) que ceux basés sur des algorithmes à clé secrète ("MAC", ou "Message Authentication Code" en anglais).

Les notations utilisées dans la suite sont les suivantes :

- 5 m_{ij} : message déterminé par l'entité i et destiné à l'entité j . Un message déterminé par une entité i pourra très bien être vide ou identique à un message déterminé par une autre entité j ($m_{i,1}=m_{j,1}$ pour $i \neq j$ et 1 donné), ou encore un cryptogramme. Dans le cas du paiement par carte PME (Porte-Monnaie Electronique), $m_{i,j}$ désignera par exemple les données de la transaction (y compris les éléments anti-rejeux).
- 10 $K_{i,j}(m)$: cryptogramme du message m , calculé par i à l'aide du système de clés K_{ij} . L'algorithme de calcul de ce cryptogramme dépend de l'application. Il n'est fait aucune restriction

15 sur l'algorithme utilisé pour le calcul de ce cryptogramme. Il pourra s'agir par exemple :

 1. d'un algorithme à clé publique (RSA, DSA, etc...) ou d'un algorithme à clé secrète (MAC-DES, etc...),
 - 20 2. d'un algorithme de signature, ou d'un algorithme de chiffrement. Dans le cas d'une signature, on suppose implicitement que le cryptogramme utilisé permet le recouvrement d'un message. Cette
 - 25 hypothèse n'est pas restrictive car on peut toujours remplacer $K_{ij}(m)$ par $K'_{ij}(m)=K_{ij}(m)||m$, où $||$ désigne la concaténation de messages.
- 30 La notation $K_{ij}(X,m)$ est considérée comme équivalente à $K_{ij}(X||m)$, dans l'hypothèse où les deux parties en présence ont convenu de la longueur de X .

- Dans la suite, le message X sera lui-même un cryptogramme $K(m')$. On appellera "encapsulation" le fait d'utiliser ainsi un cryptogramme $X=K'(m)$ comme message.
- 5 • Lorsque le cryptogramme $K_{ij}(X,m)$ est destiné à préserver l'intégrité du message, mais que les canaux qu'il doit emprunter sont contrôlés par des entités qui ont intérêt au transfert de X , on pourra avoir par exemple $K_{ij}(K(m'),m)=K(m')$
- 10 $||K'_{ij}(m)$, aucune restriction n'étant faite sur l'algorithme de calcul des cryptogrammes.

Quatre exemples de mise en oeuvre de ce procédé vont être décrits,

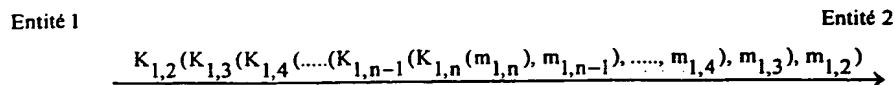
15

Exemple 1 : Encapsulation totale à la source et décapsulation progressive

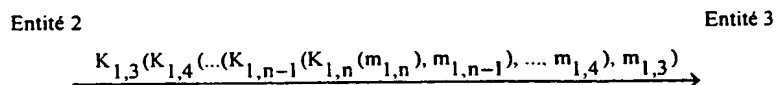
- La source élabore un message $m_{1,n}$ rassemblant les données de la transaction et calcule un premier
- 20 cryptogramme $K_{1,n}(m_{1,n})$ de ce premier message en utilisant un premier système de clés $K_{1,n}$ qu'elle partage avec la dernière $n^{\text{ième}}$ entité ; la source associe ensuite à ce premier cryptogramme un deuxième message $m_{1,n-1}$ et calcule un deuxième cryptogramme
- 25 $K_{1,n-1}(K_{1,n}(m_{1,n}),m_{1,n-1})$ de l'ensemble en utilisant un deuxième système de clés $K_{1,n-1}$ qu'elle partage avec une avant-dernière $(n-1)^{\text{ième}}$ entité, et ainsi de suite, ... ; la première entité associe au $(n-2)^{\text{ième}}$ cryptogramme précédemment obtenu un $(n-1)^{\text{ième}}$ message
- 30 $m_{1,2}$ et calcule un $(n-1)^{\text{ième}}$ cryptogramme de l'ensemble en utilisant un $(n-1)^{\text{ième}}$ système de clés $K_{1,2}$ qu'elle partage avec une deuxième entité, et la source transmet

le dernier cryptogramme calculé à travers le réseau de communication vers l'entité 2.

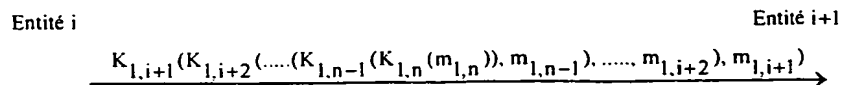
On peut schématiser cette première phase par le diagramme suivant où la flèche orientée à droite symbolise le transfert d'information entre l'entité 1 (à gauche) et l'entité 2 (à droite) :



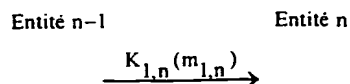
L'entité 2, qui reçoit le message de l'entité 1, réalise une décapsulation partielle de ce message à l'aide du système de clés $K_{1,2}$; elle vérifie (et conserve éventuellement) le cryptogramme qui lui est destiné (en l'occurrence la signature du message $m_{1,2}$), puis transmet à l'entité 3 le reste du message. On a donc, avec les mêmes conventions, le schéma suivant :



Ce procédé est réitéré de proche en proche jusqu'à l'entité n. Pour les entités i et i+1 intermédiaires, on a :



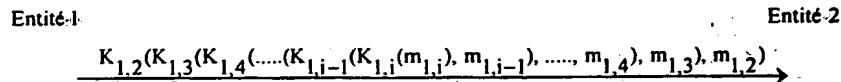
Enfin, l'avant-dernière entité (n-1) transmet au destinataire (n) le dernier cryptogramme $K_{1,n}(m_{1,n})$ et celui-ci, à l'aide du système de clés $K_{1,n}$, récupère le message qui lui était destiné :



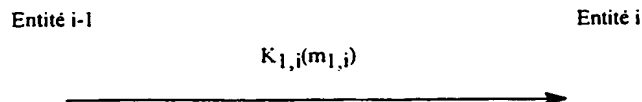
Exemple 2 : Encapsulation partagée

L'entité 1 partage un système de clés avec seulement une partie des entités se trouvant sur le chemin de communication, à savoir les entités 2, ..., i qui forment un premier groupe. L'entité i, quant à elle, partage un système de clés avec chacune des entités suivantes : i+1, i+2, ..., n et forme avec elles un second groupe.

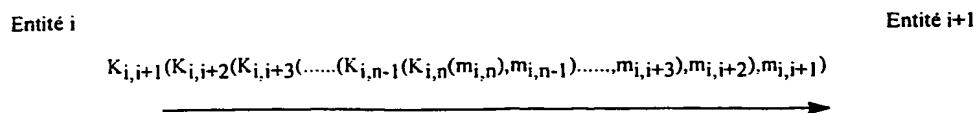
L'entité 1 élabore un message pour la dernière entité i du premier groupe, soit $m_{1,i}$ et encapsule ce message avec les systèmes de clés qu'elle partage avec chacune des entités du premier groupe, et transmet le tout à l'entité 2 :



Dans ce premier groupe, les entités décapsulent progressivement les cryptogrammes jusqu'à ce que l'avant-dernière entité i-1 transmette à la dernière entité i, le cryptogramme du message qui lui est destiné :



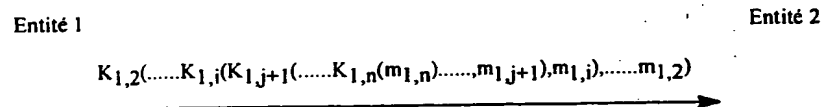
L'entité i procède alors à une encapsulation de la totalité des messages $m_{i,i+1}, m_{i,i+2}, \dots, m_{i,n}$ destinés aux entités du second groupe. Le contenu de ces messages peut dépendre du cryptogramme reçu. Le résultat de cette encapsulation est ensuite transmis selon le procédé déjà décrit, d'abord de l'entité i à l'entité i+1 :



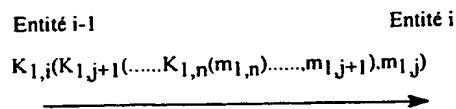
et ainsi de suite à travers les entités du second groupe jusqu'à l'avant dernière, $n-1$, qui transmet le dernier cryptogramme au destinataire n .

5 Exemple 3 : Cas général

L'entité 1 partage un système de clés avec une partie des entités se trouvant sur le chemin de communication, partie que pour la simplicité de l'exposé, on supposera être 2, ..., i , $j+1$, ..., n .
 10 L'entité 1 réalise donc une encapsulation partielle comme le montre le schéma suivant :

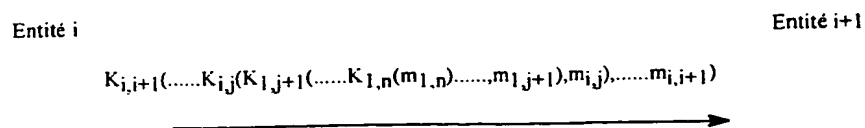


Chaque entité intermédiaire décapsule le message qu'elle reçoit à l'aide du système de clés approprié, et ceci jusqu'à l'entité i :

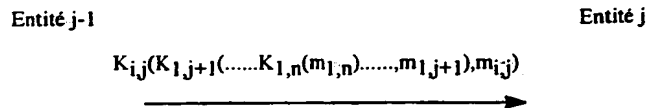


Tout acteur (ici " i " uniquement), qui, après avoir extrait le message qui lui était destiné, obtient un reste de message destiné à un acteur non adjacent sur le parcours, le réencapsule à destination de l'entité adjacente et (éventuellement) des suivantes.
 20

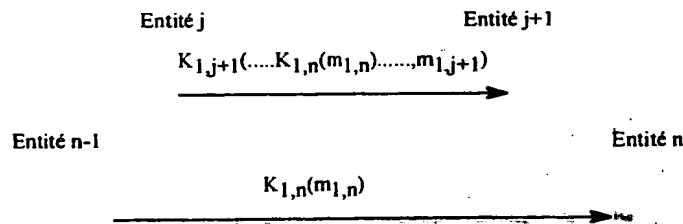
Dans cet exemple, l'entité i partage un système de clés avec chacune des entités suivantes : $i+1$, $i+2$, ..., j . L'entité i reçoit le message de $i-1$, réalise une décapsulation partielle, puis réencapsule le message obtenu à destination de $i+1$, $i+2$, ..., j .
 25



Chaque entité intermédiaire décapsule le message qu'elle reçoit à l'aide du système de clés et ceci jusqu'à l'entité j :

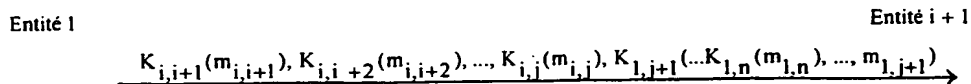


- 5 L'entité j décapsule à nouveau. Le message décapsulé est ensuite transmis de proche en proche de j+1 à n :



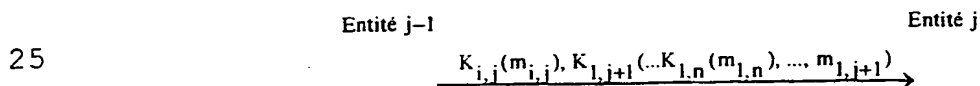
10

- On peut illustrer, dans le cadre de cet exemple, le cas particulier décrit précédemment dans lequel certains cryptogrammes $K_{i,j}(\dots)$ sont de la forme $K_{i,j}(X, m) = X, K_{i,j}(m)$. L'entité i n'encapsule pas les messages à destination de i+1, i+2, ..., j, parce que les canaux sont considérés comme sûrs et les entités impliquées n'ont pas intérêt à falsifier les messages.



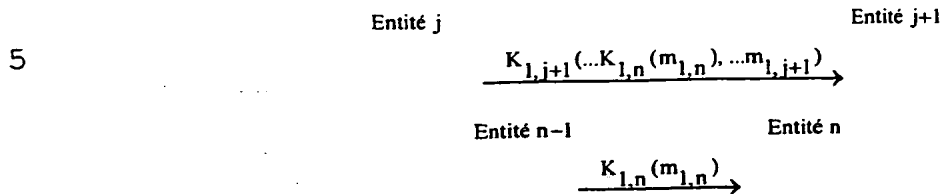
20

Chaque entité intermédiaire reçoit et contrôle le message qui lui est destiné à l'aide de son système de clés, ceci jusqu'à l'entité j.



25

L'entité j reçoit et contrôle le message qui lui est destiné. Le message est ensuite transmis de proche en proche de $j+1$ à n :



Exemple 4 : cas du porte-monnaie électronique (PME)

10 Dans cet exemple, les entités (ou les acteurs) sont :

- des cartes PME notées A,
- des points de service P, aptes à recevoir les cartes,
- des concentrateurs de points de service et leur module de sécurité MS,
- 15 • un émetteur E chargé d'émettre les cartes PME et chargé d'acquérir la monnaie électronique.

Le réseau de communication relie les points de service aux concentrateurs et ces concentrateurs à l'émetteur.

20

Par hypothèse :

- A et MS partagent un système de clés $K_{A,M}$,
- A et E partagent un système de clés $K_{A,E}$,
- A et P partagent un système de clés $K_{A,P}$.

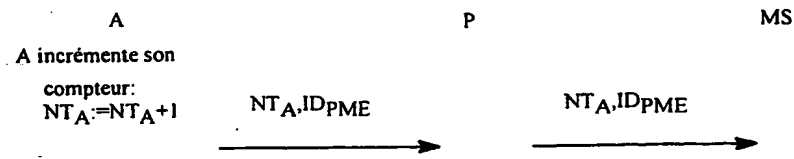
25

Les notations employées sont les suivantes :

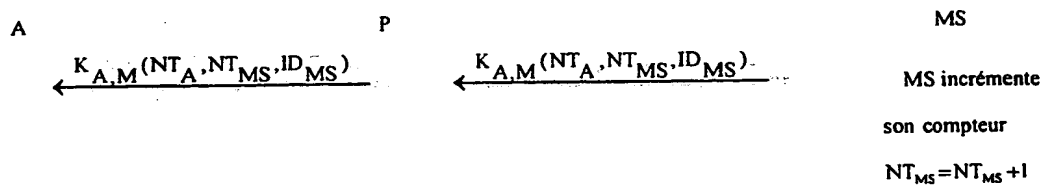
- $K(m)$ cryptogramme du message m obtenu en utilisant le système de clés K ,
- NT_A : numéro de transaction du PME A,

- NT_{MS} : numéro de transaction de MS,
- ID_{PME} : identifiant du PME,
- ID_{MS} : identifiant de MS.

- 5 Après l'étape préalable d'échange de clés, A, P et MS échangent des informations relatives au numéro de la transaction NT_A et à l'identifiant du PME :



- 10 Puis le module de sécurité communique à l'entité P son numéro de transaction NT_{MS} , après l'avoir incrémenté, ainsi que son identité ; l'identité P retransmet ces informations à l'entité A.



- 15 La carte A vérifie les données qu'elle a reçues et initialise à zéro le cumul (cumul=0).

Commence alors le cycle de consommation d'unités de service. Les opérations mises en oeuvre sont alors les suivantes :

A

P

← ordre de débit de montant m

cumul := cumul+m

calcul de la micro-transaction

$\xrightarrow{K_{A,P}(M, K_{A,M}(M, K_{A,E}(M')))}$

où $M = (m, \text{cumul}, NT_A, NT_{MS}, ID_{MS})$

et $M' = (\text{cumul}, NT_A, NT_{MS}, ID_{MS})$

P vérifie les données qui lui ont été

transmises

cumul := cumul+m

C'est ensuite le retour au début du cycle si l'utilisation du service n'est pas terminée. En fin de session de service, on a l'ultime échange suivant :

P

MS

E

5

P ne transmet à MS

que la dernière signature

$\xrightarrow{K_{A,M}(M, K_{A,E}(M'))}$

$\xrightarrow{K_{A,E}(M')}$

REVENDICATIONS

1. Procédé de réalisation d'une transaction électronique à travers un réseau de communication
5 reliant une pluralité d'entités, caractérisé en ce qu'il comprend les opérations suivantes :

a) une première entité élabore un premier message rassemblant les données de la transaction et calcule un premier cryptogramme de ce premier
10 message en utilisant un premier système de clés qu'elle partage avec une dernière ($n^{\text{ième}}$) entité ; la première entité associe ensuite à ce premier cryptogramme un deuxième message et calcule un deuxième cryptogramme de l'ensemble
15 en utilisant un deuxième système de clés qu'elle partage avec une avant-dernière ($(n-1)^{\text{ième}}$) entité ; et ainsi de suite ; la première entité associe au ($(n-2)^{\text{ième}}$) cryptogramme précédemment obtenu un ($(n-1)^{\text{ième}}$)
20 message et calcule un ($(n-1)^{\text{ième}}$) cryptogramme de l'ensemble en utilisant un ($(n-1)^{\text{ième}}$) système de clés qu'elle partage avec une deuxième entité ; la première entité transmet le dernier cryptogramme calculé à travers le réseau de
25 communication,

b) la deuxième entité reçoit ce dernier cryptogramme, utilise le système de clés approprié pour extraire du ($(n-1)^{\text{ième}}$)
cryptogramme le ($(n-1)^{\text{ième}}$) message qu'il
30 contient, et transmet le ($(n-2)^{\text{ième}}$) cryptogramme restant à la troisième entité ; et ainsi de suite ; la $n^{\text{ième}}$ entité reçoit le premier cryptogramme et utilise le système de clés

approprié pour extraire le premier message qu'il contient.

2. Procédé selon la revendication 1, dans lequel
5 le réseau de communication comprend uniquement des entités partageant une clé avec une première entité, la transaction s'effectuant alors entre la première entité, qui est la source du message et la dernière, qui est le destinataire du message.

10

3. Procédé selon la revendication 1, dans lequel le réseau de communication comprend un premier groupe d'entités constitué d'une première entité et de (i-1) autres partageant chacune un système de clés avec
15 ladite première entité, et un deuxième groupe d'entités constitué d'une première entité qui est la dernière entité du premier groupe à savoir l'entité i et de (n-i) autres, l'entité i partageant un système de clés avec chacune des (n-i) entités suivantes, ce procédé
20 comprenant deux phases successives :

- une première phase dans laquelle le message élaboré par la première entité du premier groupe est transmis à la i^{ème} entité du premier groupe conformément aux opérations a) et b) de la
25 revendication 1,
- une seconde phase dans laquelle le message extrait par la première entité du second groupe est transmis à la dernière entité du second groupe conformément aux opérations a) et b) de la revendication 1.

30

4. Procédé selon la revendication 1, dans lequel le réseau de communication comprend un premier groupe d'entités constitué d'une première entité et de (i-1)

autres partageant chacune un système de clés avec ladite première entité, un deuxième groupe d'entités constitué d'une première entité, qui est la dernière entité du premier groupe et $(j-i+1)$ autres partageant
 5 chacune un système de clés avec ladite première entité du deuxième groupe, un troisième groupe d'entités constitué d'une première entité qui est la dernière entité du deuxième groupe et de $(n-j)$ autres, les $(n-j+1)$ entités de ce troisième groupe partageant
 10 chacune un système de clés avec la première entité du premier groupe, ce procédé étant caractérisé en ce que :

- la première entité du premier groupe effectue les opérations a) de la revendication 1, avec
 15 les systèmes de clés qu'elle a en commun avec chacune des autres entités du premier et du troisième groupe,
- les entités du premier groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) de la revendication 1,
 20
- la première entité du deuxième groupe effectue les opérations a) de la revendication 1 avec les systèmes de clés qu'elle a en commun avec chacune des autres entités du deuxième groupe,
- 25 - les entités du deuxième groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) de la revendication 1,
- les entités du troisième groupe décryptent les cryptogrammes qu'elles reçoivent conformément
 30 aux opérations b) de la revendication 1.

5. Procédé selon la revendication 1 dans lequel, la première entité i d'un groupe calcule un

cryptogramme des messages destinés aux autres entités $i+1, i+2, \dots, j$ du groupe, sans les encapsuler, chaque entité $i+1, i+2, \dots, j$ reçoit et contrôle le message qui lui est destiné à l'aide de son système de clé
 5 partagé avec i .

6. Procédé selon la revendication 1, dans lequel la transaction électronique est un paiement, les entités étant constituées par des cartes (A), des
 10 points de service (P) aptes à recevoir lesdites cartes (A), des concentrateurs de points de service équipés d'un module de sécurité (MS) et reliés aux points de service et un émetteur (E) chargé d'émettre des cartes de type paiement électronique et chargé d'acquérir la
 15 monnaie électronique, le réseau de communication reliant des points de service (P) aux concentrateurs et ces concentrateurs à l'émetteur, chaque carte (A) partageant avec un module de sécurité (MS) un système de clés $K_{A,M}$, chaque carte A partageant également avec
 20 l'émetteur (E) un système de clés $K_{A,E}$, chaque carte (A) partageant avec un point de service (P) un système de clés $K_{A,P}$.

7. Procédé selon la revendication 6, dans lequel :

25 a) la carte (A) :

- calcule un message (M') à destination de l'émetteur (E), ce message comprenant le cumul des montants payés, le numéro (NT_A) de la transaction, le numéro de transaction (NT_{MS}) du
 30 module de sécurité (MS) auquel le point de service est relié, et l'identifiant (ID_{MS}) de ce module de sécurité,

- calcule un premier cryptogramme $K_{A,E}(M')$ de ce message en utilisant le système de clés $K_{A,E}$ qu'elle partage avec l'émetteur,
 - ajoute à ce premier cryptogramme un message (M) contenant le montant de la transaction (m), le cumul, les numéros (NT_A , NT_{MS}) et l'identifiant (ID_{MS}),
 - encapsule le résultat dans un deuxième cryptogramme $K_{A,M}(M, K_{A,E}(M'))$ utilisant le système de clés $K_{A,M}$ qu'elle partage avec le module de sécurité (MS),
 - ajoute à ce deuxième cryptogramme, le message M,
 - encapsule le résultat dans un troisième cryptogramme $K_S(M, K_{A,M}(M, K_{A,E}(M')))$, en utilisant le système de clés $K_{A,P}$,
 - transmet ce troisième cryptogramme au point de service (P),
- b) le point de service (P) décapsule le cryptogramme reçu à l'aide du système de clés $K_{A,P}$, récupère et vérifie le message M, et enregistre $K_{A,M}(M, K_{A,E}(M'))$, le procédé étant répété si l'utilisation du service n'est pas terminée,
- c) en fin d'utilisation du service le point de service (P) retransmet le dernier $K_{A,M}(M, K_{A,E}(M'))$ au module de sécurité (MS),
- d) le module de sécurité (MS) décapsule le cryptogramme reçu à l'aide du système de clés $K_{A,M}$, récupère le message (M) et transmet $K_{A,E}(M')$ à l'émetteur,
- e) l'émetteur (E) décapsule le cryptogramme reçu à l'aide du système de clés $K_{A,E}$ et extrait le message (M') qui lui était destiné.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)